

12/17/99

Jc685 U.S. PTO

# UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.

1614.1020

First Named Inventor or Application Identifier:

Kenichi YAMAMOTO et al.

Express Mail Label No.

Jc518 U.S. PTO

12/17/99

**APPLICATION ELEMENTS**

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO:

**Assistant Commissioner for Patents  
Box Patent Application  
Washington, DC 20231**

1. ☒ Fee Transmittal Form
2. ☒ Specification, Claims & Abstract ..... [ Total Pages: 25 ]
3. ☒ Drawing(s) (35 USC 113) ..... [ Total Sheets: 9 ]
4. ☒ Oath or Declaration ..... [ Total Pages: 4 ]
  - a. ☒ Newly executed (original or copy)
  - b. ☐ Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional with Box 17 completed)
    - i. ☐ **DELETION OF INVENTOR(S)**  
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation by Reference (usable if Box 4b is checked)  
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ Microfiche Computer Program (Appendix)
7. ☐ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
  - a. ☐ Computer Readable Copy
  - b. ☐ Paper Copy (identical to computer copy)
  - c. ☐ Statement verifying identity of above copies

**ACCOMPANYING APPLICATION PARTS**

8. ☒ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(b) Statement (when there is an assignee) [ ] Power of Attorney
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. ☐ Small Entity Statement(s) [ ] Statement filed in prior application, status still proper and desired.
15. ☒ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. ☐ Other:

**17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information:**[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No: 1**18. CORRESPONDENCE ADDRESS**

STAAS & HALSEY LLP  
Attn: H. J. Staas  
700 Eleventh Street, N.W., Suite 500  
Washington, DC 20001

Telephone: (202) 434-1500  
Facsimile: (202) 434-1501

<b>NEW APPLICATION FEE TRANSMITTAL</b>		Attorney Docket No.	1614.1020
		Application Number	
		Filing Date	December 17, 1999
AMOUNT ENCLOSED	\$ 800.00	First Named Inventor	Kenichi YAMAMOTO et al.

**FEE CALCULATION** (fees effective 10/01/97)

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
	TOTAL CLAIMS	10 - 20 =	0	X \$ 18.00 =	\$ 0.00
	INDEPENDENT CLAIMS	2 - 3 =	0	X \$ 78.00 =	0.00
	MULTIPLE DEPENDENT CLAIMS (any number; if applicable)			+ \$240.00 =	0.00
	<b>BASIC FILING FEE</b>				+ 760.00
	Total of above Calculations =				\$ 760.00
	Surcharge for late filing fee, Statement or Power of Attorney (\$130.00)				+ 0.00
	Reduction by 50% for filing by small entity (37 CFR 1.9, 1.27 & 1.28).				- 0.00
	<b>TOTAL FILING FEE =</b>				\$ 760.00
	Surcharge for filing non-English language application (\$130.00; 37 CFR 1.52(d))				+ 0.00
	Recordation of Assignment (\$40.00; 37 CFR 1.21(h)(1))				+ 40.00
	<b>TOTAL FEES DUE =</b>				\$ 800.00

**METHOD OF PAYMENT**

- ☒ Check enclosed as payment.
- ☐ Charge "TOTAL FEES DUE" to the Deposit Account No., below.
- ☐ No payment is enclosed and no charges to the Deposit Account are authorized at this time.

**GENERAL AUTHORIZATION**

- ☒ If the above-noted "AMOUNT ENCLOSED" is not correct, the Commissioner is hereby authorized to credit any overpayment or charge any additional fees necessary to:

Deposit Account No.


19-3935

Deposit Account Name

STAAS &amp; HALSEY LLP

- ☒ The Commissioner is also authorized to credit any overpayments or charge any additional fees required under 37 CFR 1.16 (filing fees) or 37 CFR 1.17 (processing fees) during the prosecution of this application, including any related application(s) claiming benefit hereof pursuant to 35 USC § 120 (e.g., continuations/divisionals/CIPs under 37 CFR 1.53(b) and/or continuations/divisionals/CPAs under 37 CFR 1.53(d)) to maintain pendency hereof or of any such related application.

**SUBMITTED BY: STAAS & HALSEY LLP**

Typed Name	H. J. Staas	Reg. No.	22,010
Signature		Date	December 17, 1999

SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

BE IT KNOWN THAT WE, Kenichi Yamamoto, a citizen of Japan residing at Kawasaki-shi, Kanagawa, Japan, Hideaki Okada, a citizen of Japan residing at Maebashi-shi, Gunma, Japan, Teruo Nakazawa, a citizen of Japan residing at Maebashi-shi, Gunma, Japan and Hideki Mikamoto, a citizen of Japan residing at Ota-ku, Tokyo, Japan have invented certain new and useful improvements in

INFORMATION PROVIDING SYSTEM AND  
METHOD FOR PROVIDING INFORMATION

of which the following is a specification : -

TITLE OF THE INVENTION

INFORMATION PROVIDING SYSTEM AND METHOD  
FOR PROVIDING INFORMATION

5 BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention generally relates to information providing systems and methods for providing information that provide information via a network, and more particularly to an information providing system and a method for providing information that can provide information required by users while user information about the users accessing the provided information can be managed.

15 Recently, especially in the Internet industry using computers, the Internet has increased its business value yearly and information providing services are frequently performed for authorized users through the World Wide Web (hereinafter called  
20 WWW). In this case, authentication technologies are applied so as to confirm whether a user is authorized to use the information providing services. However, when a duplicate use of the same user ID from two different terminals is attempted to connect to the  
25 same server at the same time, the duplicate use of the user ID is authenticated. Also, when a user's terminal is not capable of communicating with a server after a user ID is authenticated, the user is not able to access the server from another terminal.  
30 Problems of the authentication technologies such as those mentioned above are occurring. Accordingly, current authentication technologies at servers are not enough to manage user access information. It is desired to provide a system in which a server can  
35 recognize connection conditions of authenticated users' client terminals (hereinafter referred to as clients).

## 2. Description of the Related Art

A conventional user authentication on the WWW will now be explained.

FIG.1 is a schematic illustration of a WWW  
5 network structure.

In FIG.1, the WWW network structure includes a server 200 to provide information, clients 2201 through 220n for users to access the server 200 (hereinafter a reference number 220 is used for a  
10 client as a general term) and a public network 210 such as the Internet.

In order to be provided information from the server 200, a user connects a client 220 to the server 200 via the public network 210. After the  
15 client 220 is connected to the server 200, the server 200 starts to provide information in accordance with user's requests.

A conventional method for managing user access information about a user that uses a client  
20 connecting to a server on the WWW will now be explained.

FIG.2 is a flowchart showing an example of a conventional WWW user access management.

For example, in order to connect a client  
25 2201 to a server 200, the user A accesses a screen 1 provided by the server 200 (step S1). The server 200 sends an authentication screen for authenticating the user A to the client 2201 (step S2). The user A inputs a user ID and a password to the authentication  
30 screen displayed at the client 2201 (step S3). The server 200 authenticates the user A based on the user ID and the password sent from the client 2201 (step S4) and registers the user ID with a session ID (for example, '123') assigned for the user ID to a  
35 management table (step S5). Also, the server 200 sets the session ID in the screen 1 and sends the screen 1 to the client 2201 (step S6). At the client

2201, the screen 1 sent from the server 200 is displayed (step S7). In accordance with a user's request, the client 2201 makes a screen 2 request of the server 200 after the client 2201 sends the  
5 session ID set in the screen 1 to access screen 2 next (step S8). The server 200 confirms the session ID ('123') in the management table based on the request from the client 2201 (step S9). In this case, the session ID ('123') is already registered for the  
10 user ID. Hence, the server 200 sends a screen 2 to the client 2201 (step S10). The screen 2 is received and displayed at the client 2201.

It is assumed that the user A or another user attempts to connect another client 2202 to the  
15 server 200 by using the user ID and the password for the user A.

The client 2202 accesses the screen 1 provided by the server 200 (step S12). The server 200 sends the authentication screen to the client  
20 2202 (step S13). When the authentication screen is displayed at the client 2202, the user inputs the user ID and the password for the user A and the client 2202 sends this information to the server 200. The server 200 confirms the user ID and the password  
25 received from the client 2202 (step S15). That is, the server 200 checks whether a session ID for the user ID is registered in the management table or not. In this case, the session ID for the user ID is already registered as '123' and is still being used  
30 on the WWW. Hence, the server 200 sends an error message to the client 2202 (step S16). The error message is displayed at the client 2202 (step S17). The message shows the user that no information will be provided. And the access by the user A is denied.

35 In the conventional user access management on the WWW, the server 200 allows a duplicate login of the user A to obtain information service that is

only for authenticated users while the user A is still being provided information from the server 200.

The Internet was originally constructed such that any user connecting to the Internet was  
5 allowed to share all information provided by servers connecting to the Internet. In this feature of the Internet, generally, the servers do not have to monitor a screen flow of clients or the like. Thus, some servers do not have a function such as a  
10 function for monitoring the screen flow.

In the conventional user access management on the WWW as shown in FIG.2, it is assumed that the user A accesses another home page provided by another server and a browser of the client 2201 flows to  
15 another screen while the user A is provided information by the server 200 on the WWW. In this case, the server 200 does not have a function for monitoring the screen flow of the client 220. Thus, the session ID for the user A remains in the  
20 management table of the server 200. After that, the user ID and the password for the user A can not be allowed to access the server 200.

Also, even if the client 2201 used by the user A is not able to communicate with the server 200  
25 because a fault occurs during the session established with the server 200, the server 200 does not have any means to recognize an abnormal state of the client 2201. As a result, the session between the server 200 and the client 2201 remains in the management  
30 table. Thus, the user ID and the password for the user A can not be used to access the server 200.

#### SUMMARY OF THE INVENTION

It is a general object of the present  
35 invention to provide information providing systems and methods for providing information that provide information via a network in which the above-

mentioned problems are eliminated.

A more specific object of the present invention is to provide an information providing system and a method for providing information that  
5 can provide information required by users while user information about the users accessing the provided information can be managed.

The above objects of the present invention are achieved by an information providing system  
10 including: a condition notifying part, which is activated in a user terminal connecting to the information providing system via a network, for notifying of a condition of the user terminal; a providing part for providing the condition notifying  
15 part to the user terminal with information that is in accordance with a request of the user terminal; and a session management part managing session information to provide information to the user terminal in accordance with the condition of the user terminal  
20 that is notified by the condition notifying part activated in the user terminal, so that a session between the information providing system and the user terminal is established when the user is authenticated in accordance with authentication  
25 information from the user terminal and the session information managed by the session management part.

According to the present invention, the session management part manages the session, which is  
30 used to provide information to the user, in accordance with the condition of the user terminal that is notified by the condition notifying part activated in the user terminal. Therefore, it is possible to manage the session in accordance with the condition of the user terminal.

35 In addition, the above objects of the present invention are achieved by a method for providing information including the steps of (a)



notifying of a condition of a user terminal, which  
notifying is activated in the user terminal  
connecting to a server via a network; (b) providing  
the step (a) from the server to the user terminal  
5 with information that is in accordance with a request  
of the user terminal; and (c) managing session  
information in the server to provide information to  
the user terminal in accordance with the condition of  
the user terminal notified by the step (a) activated  
10 in the user terminal, so that a session between the  
server and the user terminal is established when the  
user is authenticated by the server in accordance  
with authentication information from the user  
terminal and the session information managed in the  
15 step (c).

#### BRIEF DESCRIPTION OF THE DRAWINGS

Other objects, features and advantages of  
the present invention will become more apparent from  
20 the following detailed description when read in  
conjunction with the accompanying drawings, in which:

FIG.1 is a schematic illustration of a WWW  
network structure;

FIG.2 is a flowchart showing an example of  
25 a conventional user access management on the WWW;

FIG.3 is a hardware configuration of a  
server on the WWW as an information providing system  
according to an embodiment of the present invention;

FIG.4 is a block diagram showing a  
30 functional construction of a server 100;

FIG.5 is a diagram showing a session  
establishment between the server 100 and a client  
400;

FIG.6 is a flowchart showing the session  
35 management in a normal case;

FIG.7 is a flowchart explaining the  
session management method in the case in which there

is no communication from a client according to the embodiment of the present invention; and

FIG.8 is a diagram showing a session establishment between the server 100 and the client  
5 400; and

FIG.9 is a flowchart explaining the modification of the session management method in the case in which there is no communication from a client according to the modification of the embodiment of  
10 the present invention.

#### DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG.3 is a hardware configuration of a server on the WWW as an information providing system  
15 according to an embodiment of the present invention.

In FIG.3, the server providing information on the WWW includes a CPU 11 to execute a session management program that will be explained later, a memory unit 12 to temporarily store the program and  
20 data, a communication unit 13 to control sending/receiving of data to/from outside, an input unit 14 to control input data, a display unit 15 to control display information, a storage device 16 to load the program to be executed and a CD-ROM drive  
25 unit 17 to access a CD-ROM 19, all of which are connected to a bus. Programs according to an information providing process are provided by the CD-ROM 19. That is, programs read from the CD-ROM 19 are installed into the storage device 16 through the  
30 CD-ROM drive unit 17. It should be noted that a recording medium is not limited to a CD-ROM, but other computer-readable recording media such as a magnetic disk, a magnetic tape, an optical disk, an optical magnetic disk, a semiconductor memory or the  
35 like may be used.

Also, hardware configurations of the clients 220 connecting to the server 200 are the same

as that of the server 200.

FIG.4 is a block diagram showing a functional construction of a server 100.

The server 100 as an information providing  
5 system includes a communication protocol TCP/IP  
(Transmission Control Protocol / Internet Protocol)  
21 to control data from/to the communication unit 13  
in FIG.3, a daemon 22 to manage user information, a  
CGI (Common Gateway Interface) 23 to associate with  
10 external programs, an HTTP (HyperText Transfer  
Protocol) 24 to display a screen file on a browser, a  
recording medium 25 to store tables or files needed  
by the system, a management table 26 to authenticate  
users, an HTML (HyperText Mark-up Language) area 27,  
15 screen files 28 to be displayed on the browser, an  
input component 29 to control input data from the  
input unit 14, a display component 30 to control  
display information, a timer 31 to clock a  
predetermined time, and a monitoring applet 32 to be  
20 activated at a client 220.

The client 220 is able to communicate with  
the server 100 by processing a Socket() command.  
After the Socket() command is processed, the daemon  
22 in the server 100 authenticates a user ID and a  
25 password sent from the client 220 in accordance with  
the management table 26. Thus, a session between the  
client 220 and the server 100 is established.

The screen 28 including the information to  
be provided to the user is transmitted to the client  
30 220 on the HTTP 24 on the TCP/IP 21 and is displayed  
on a browser of the client 220 used by the user.

The monitoring applet 32 is transmitted to  
the client 220 by attaching to a first screen file 28  
when the session is established. The monitoring  
35 applet 32 installed into the client 220 starts to  
monitor a screen state of the browser at the client  
220 such as a screen flow and sends screen event

information indicating the screen state to the server 100 at every screen flow. The monitoring applet 32 in the client 220 executes the CGI 23 in the server 100 if necessary so as to update the management table 26 via the CGI 23.

The timer 31 starts simultaneously when the session is established and is used to confirm at the predetermined time whether the user is still using the information provided by the server 100. The session is released when the access of the user on the session is recognized before the predetermined time.

According to the embodiment of the present invention, a session establishment between the server and a client on an upper layer of the TCP/IP and a monitor process of the client, will now be explained with reference to FIG.5.

FIG.5 is a diagram showing a session establishment between the server 100 and a client 400. The functional construction of the server 100 as an information providing system is as shown in FIG.4.

The client 400 includes a communication protocol TCP/IP 61, an HTTP 64 to display a screen file on a browser, a browser area 67, screen files 281 and 282 to be displayed on the browser, an input component 69 to control input data, a display component 70 to control display information and a monitoring applet 72 to monitor screen flow on the browser.

The client 400 attempts to connect with the server 100 by establishing a socket() 41 on the TCP/IP 61 via the public network. The server 100 sends an authentication screen to obtain a user ID and a password from the client 400 and to authenticate the user. After the authentication, the server 100 provides a session ID in the first screen

281 which initially provides information and sends the screen 281 with the monitoring applet 32.

5       The screen 281 is transmitted to the client 400 via a route 54, developed in the browser area 67 and displayed on the browser while the monitoring applet 32 attached to the screen 281 is installed into the client 400 so as to be the monitoring applet 72 and establishes a session 53 by the daemon 22 of the server 100. After that, the  
10       monitoring applet 72 sends the screen event information to the server 100 through the session 53 until the session is released. That is, the session 53 is established between the server 100 and client 400 on the TCP/IP and information about the session  
15       53 is managed by the daemon 22 of the server 100 and the monitoring applet 72 of the client 400. In addition, a state in which the monitoring applet 72 of the client 400 can respond to a request from the server 100 is established.

20       When the browser flows to a screen 282 from the screen 281 at the client 400, the monitoring applet 72 sends the screen event information indicating the screen flow to the daemon 22 of the server 100 via the session 53 while the screen 282  
25       received through a route 55 is developed in the browser area 67 and displayed on the browser.

      On the other hand, when the client 400 accesses another server 300 and the browser flows to another screen provided by the server 300, the  
30       monitoring applet 72 sends the screen event information indicating the screen flow by switching to another server to the daemon 22 of the server 100. Then, the daemon 22 initializes session information about the client 400 stored in the management table  
35       26 so that the session is released.

      A session management in a normal case will now be explained.

FIG.6 is a flowchart showing the session management in a normal case.

In FIG.6, functional constructions of clients 4001 and 4002 are the same as that of the client 400 shown in FIG.5

In FIG.6, when the client 4001 operated by a user A attempts to access the first screen 1 in order to connect to the server 100 (step S21), the server 100 sends an authentication screen to the client 400 in order to authenticate the user A (step S22). At the client 4001, the user A inputs a user ID (for example, 'AAA') and a password to the authentication screen received from the server 100 (step S23). The server 100 authenticates the user A based on the user ID and the password received from the client 4001 (step S24). The server 100 assigns a session ID (for example, '123') to the user ID 'AAA' and registers this information in the management table 26 (step S25). The server 100 provides the session ID '123' in the screen 1 and sends the screen 1 with the monitoring applet 32 to the client 4001 (step S26).

The screen 1 sent from the server 100 is displayed at the client 4001 (step S27). In addition, the monitoring applet 32 is installed into the client 4001 so as to be the monitoring applet 72. The monitoring applet 72 starts to establish a session having the session ID '123' with the server 100 (step S28).

After the session is established, the monitoring applet 72 monitors events concerning the screen flow at the client 4001, including user operations of indicating a URL, clicking a back button or a forward button and so on.

When the browser of the client 4001 flows to another screen, the monitoring applet 72 sends the screen event information indicating screen flow by

switching to another server to the server 100 (step S29).

When the server 100 receives the screen event information indicating screen flow by switching  
5 to another server from the client 4001, the CGI  
executes the daemon 22 so that the daemon 22 deletes  
the user ID 'AAA' and the session ID '123' for the  
user A in the management table 26 (step S30). Thus,  
the session between the server 100 and the client 400  
10 is released.

It is assumed that the user A attempts to obtain information from another client 4002.

The user A accesses the first screen 1 provided by the server 100 from the client 4002 (step  
15 S32). The server 100 sends the authentication screen  
to the client 4002 in order to authenticate the user  
A (step S33). The user A inputs the user ID and the  
password to the authentication screen displayed at  
the client 4002 (step S34). The server 100  
20 authenticates the user A based on the user ID and the  
password received from the client 4002 (step S35) and  
registers the user ID 'AAA' and a new session  
ID '456' to the management table 26 (step S36).  
Subsequently, the server 100 provides the session  
25 ID '456' in the screen 1 and sends the screen 1 with  
the monitoring applet 32 to the client 4002 (step  
S37).

The client 4002 displays the screen 1 sent from the server 100 (step S38). The monitoring  
30 applet 72, which is installed into the client 4002 by  
the monitoring applet 32 sent with the screen 1 from  
the server 100, establishes a session having the  
session ID '456' with the server 100 (step S39).

After that, if the user ID and the  
35 password for the user A are used from other client to  
access the server 100, the server 100 can recognize,  
by using the management table 26, that the user ID

for the user A is already registered with the session having the session ID '456' so that the server 100 does not authenticate the user A. Thus, the duplicate login can be prevented.

5                   The session management method in a case in which there is no communication from a client after a session establishment, that is, the client is in a non-communication state which is not abnormal (a sleep condition) or the client is in another non-communication state caused by a fault (an abnormal condition), will now be explained.

10                   FIG.7 is a flowchart explaining the session management method in the case in which there is no communication from a client according to the embodiment of the present invention.

15                   In FIG.7, the user A accesses the screen 1 provided by the server 100 from the client 400 (step S41). The server 100 sends the authentication screen to the client 400 in order to authenticate the user A (step S42). The user ID (for example, 'AAA') and the password input by the user A to the authentication screen are transmitted to the client 400 (step S43).

20                   The server 100 authenticates the user A based on the user ID 'AAA' and the password received from the client 400 (step S44) and registers the user ID 'AAA' and a session ID (for example, '123') assigned for the user ID in the management table 26 (step S45). In addition, the server 100 starts an existence check timer to check a state of the client 400 at a predetermined time (step S46). Then, the server 100 sends the screen 1, in which the session ID '123' is provided, with the monitoring applet 32 to the client 400.

30                   The client 400 displays the screen 1 on the display unit 15 (step S48) and the monitoring applet 72 establishes a session having the session ID '123' with the server 100 (step S49).



After that, it is assumed that the client 400 is in the sleep condition.

In this case, when the existence check timer is out after the predetermined time, the server  
5 100 sends existence check data to the client 400  
(step S50). In client 400, the monitoring applet 72  
sends existence response data to respond to the  
existence check data received from the server 100  
(step S51). The server 100 confirms a normal  
10 operation of the client 400 by receiving the  
existence response data from the client 400 (step  
S52).

The client 400 accesses a screen 2  
provided by the server 100, with the session ID '123'  
15 as an access key (step S53). The server 100 confirms  
that the user A is already registered, by searching  
the user ID 'AAA' stored in the management table 26  
by the session ID '123' (step S54). The server 100  
starts the existence check timer in order to monitor  
20 the client 400 at the predetermined time (step S55)  
and then the screen 2 is sent to the client 400 (step  
S56).

After that, it is assumed that an abnormal  
condition occurs to the client 400 so that the client  
25 400 is unable to communicate with the server 100.

The server 100 sends the existence check  
data to the client 400 after the existence check  
timer passes the predetermined time (step S58). In  
this case, it is impossible for the client 400 to  
30 respond to the existence check data from the server  
100 because the monitoring applet 72 may be destroyed.  
Hence, the server 100 can not receive the existence  
response data from the client 400. As a result, the  
server 100 deletes the user ID 'AAA' and the session  
35 ID '123' in the management table 26. Then, the  
session ID '123' is released (step S59).

In the method mentioned above, the server

100 can monitor the state of the client 400. In the case in which there is no communication with the client 400, the server 100 can check whether the client 400 is in the sleep condition or in the  
5 abnormal condition and can perform in accordance with the condition of the client 400.

A modification of the session management method in a case in which a client does not establish a session with the server 100 on the upper layer of  
10 the TCP/IP and the client sends a state of the client to the server 100 at the predetermined time on the other hand, will now be explained.

FIG.8 is a diagram showing a session establishment between the server 100 and the client  
15 400.

FIG.8, parts that are the same as those shown in the previously described figures are given the same reference numbers.

The client 400 attempts to connect to the  
20 server 100 by establishing a socket() 41 on the TCP/IP 61 via the public network. The server 100 sends the authentication screen to obtain a user ID and a password from the client 400 and to authenticate the user A. After the authentication,  
25 the server 100 provides a session ID in the first screen 281 which is information initially provided and sends the screen 281 with the monitoring applet 32.

The screen 281 is transmitted to the  
30 client 400 via the route 54, developed in the browser area 67 and displayed on the browser while the monitoring applet 32 attached to the screen 281 is installed into the client 400 so as to be the monitoring applet 72 and establishes a session 53  
35 with the daemon 22 of the server 100. After that, the monitoring applet 72 sends the screen event information to the server 100 through the session 53

until the session is released. .

When the browser flows to a screen 281 provided by the server 100 at the client 400, the monitoring applet 72 notifies the event of screen  
5 change to the server 100 by executing the CGI 22 of the server 100 through the session 53 while the screen 281 received from the server 100 through the route 55 is developed in the browser area 67 and displayed on the browser.

10 When the browser flows to another screen provided by another server 300 at the client 400, the monitoring applet 72 sends the screen event information indicating the screen flow by switching to another server to the server 100. The daemon 22  
15 of the server 100 deletes information about the user A in the management table 26 and releases the session 53.

In addition, the server 100 uses the timer 31 to monitor the client 400 by executing the daemon  
20 22 at the predetermined time.

The modification of the session management method in a case in which there is no communication from the client 400 will now be explained.

FIG.9 is a flowchart explaining the  
25 modification of the session management method in the case in which there is no communication from a client according to the modification of the embodiment of the present invention.

In FIG.9, the user A from the client 400  
30 accesses the screen 1 provided by the server 100 (step S61). The server 100 sends the authentication screen to the client 400 in order to authenticate the user A (step S62). The user ID (for example, 'AAA') and the password input by the user A to the  
35 authentication screen are transmitted to the client 400 (step S63).

The server 100 authenticates the user A

based on the user ID 'AAA' and the password received from the client 400 (step S64). Subsequently, the server 100 registers the user ID 'AAA' with a session ID '123' assigned for the user A, and sets ON to both  
5 a login flag and an existence flag (step S65) in the management table 26. In addition, the server 100 starts the existence check timer to monitor the client 400 at the predetermined time (step S66). Moreover, the server 100 provides the session  
10 ID '123' in the screen 1 and sends the screen 1 with the monitoring applet 32 to the client 400 (step S67).

The screen 1 is displayed on the browser of the client 400 (step S68). The monitoring applet 32 is installed in the client 400 so as to be the  
15 monitoring applet 72. The monitoring applet 72 starts to send existence report data (step S69).

The CGI 23 is executed by receiving the existence report data so as to update the management table 26 (step S70). Also, the server 100 checks the  
20 existence flag in the management table 26 every time when the existence check timer passes the predetermined time (step S71). Then, the server 100 resets the existence check timer (step S72).

It is assumed that the client 400 is  
25 unable to communicate with the server 100 because the abnormal condition occurs to the client 400. When the server 100 does not receive the existence report data from the client 400 after the existence timer passes the predetermined time, the server 100  
30 determines that the abnormal condition occurs to the client 400 (step S73). Hence, the server 100 sets OFF to both the login flag and the existence flag for the user A in the management table 26.

If the browser flows to another screen  
35 provided by another client at the client 400, the monitoring applet 72 sends the screen event information to the server 100. The server 100 sets

OFF to the existence flag in the management table 26 and releases the session having the session ID '123' with client 400.

As mentioned above, while the server 100  
5 is able to confirm the existence of the client 400 used by the user A on the established session, the server 100 does not allow the duplicate login of the user A because the management table 26 shows the existence of the client on the session. Therefore,  
10 the information providing system according to the present invention can prevent a server from duplicating authentication of the same user.

In addition, the problems in the conventional system such that the server rejects an  
15 access from the user when the client attempts to access the server after the browser at the client flows to another screen provided by another server or when a different client attempts to access the server by the same user after the abnormal condition occurs  
20 to the current client, can be eliminated by using the existence check timer at the server and the monitoring applet at the clients. Thus, it is possible for the user to be authenticated and to obtain information provided by the server in any case  
25 mentioned above.

The information providing system according to the present invention is not limited to application to servers only for the WWW associating with public networks, but can apply to a system such  
30 as an Intranet or the like that is an information system using an enterprise LAN system.

The present invention is not limited to the specifically disclosed embodiments, variations and modifications, and other variations and  
35 modifications may be made without departing from the scope of the present invention.

The present application is based on

Japanese Priority Application No. 10-365589 filed on December 22, 1998, the entire contents of which are hereby incorporated by reference.

WHAT IS CLAIMED IS:

5

1. An information providing system  
comprising:

10 a condition notifying part, which is  
activated in a user terminal connecting to said  
information providing system via a network, for  
notifying of a condition of the user terminal;

15 a providing part for providing the  
condition notifying part to the user terminal with  
information that is in accordance with a request of  
the user terminal; and

20 a session management part for managing  
session information to provide information to the  
user terminal in accordance with the condition of the  
user terminal that is notified by the condition  
notifying part activated in the user terminal,

25 so that a session between the information  
providing system and the user terminal is established  
when the user is authenticated in accordance with  
authentication information from the user terminal and  
the session information managed by said session  
management part.

30

2. The information providing system as  
claimed in claim 1, wherein said session management  
part is comprised of a first management program; and

35 said condition notifying part, which is  
always activated in the user terminal, comprises a  
terminal session establishing part for establishing a  
session, which is used to notify of the condition, by

the first management program.

5

3. The information providing system as claimed in claim 1, wherein said session management part is comprised of a second management program that is activated by an execution indication from outside  
10 and comprises a condition information management part for managing condition information indicating a condition of the user terminal; and

said condition notifying part activated in the user terminal comprises a condition information  
15 providing part providing the execution indication and the condition information indicating the condition of the user terminal to the second management program,

so that said session management part manages a session, which is used to provide  
20 information to the user terminal, in accordance with the condition information managed by the condition information management part that is activated by the execution indication from said condition notifying part.

25

4. The information providing system as  
30 claimed in claim 1, wherein said condition notifying part activated in the user terminal comprises:

an event monitoring part for monitoring an event concerning request information sent from the user terminal to another system; and

35 an event notifying part for notifying said session management part of the event concerning request information, which is sent from the user



terminal to another system, when the event is detected,

so that said session management part releases the session when the event is notified from  
5 the event notifying part of the user terminal.

10 5. The information providing system as claimed in claim 1, wherein said session management part comprises a confirmation part for sending a confirmation notification in a predetermined period to check whether the user terminal is connected  
15 through the session so that said session management part manages the session in accordance with a response from the user terminal to the confirmation notification; and  
said condition notification part activated  
20 in the user terminal comprises a response part for sending a response notification indicating whether the user terminal is connected through the session or not, to the session management part in response to the confirmation notification sent from the session  
25 management part.

30 6. The information providing system as claimed in claim 3, wherein said session management part manages the session based on whether the condition information is provided from the user terminal within a predetermined period or not.  
35

7. A method for providing information comprising the steps of:

- 5 (a) notifying of a condition of a user terminal, which notifying is activated in the user terminal connecting to a server via a network;
- (b) providing the step (a) from the server to the user terminal with information that is in accordance with a request of the user terminal; and
- 10 (c) managing session information in the server to provide information to the user terminal in accordance with the condition of the user terminal notified by the step (a) activated in the user terminal,
- 15 so that a session between the server and the user terminal is established when the user is authenticated by the server in accordance with authentication information from the user terminal and the session information managed in the step (c).

20

8. The method as claimed in claim 7,  
25 wherein said step (a) activated in the user terminal comprises the steps of:

- (f) monitoring an event concerning request information sent from the user terminal to another system; and
- 30 (g) notifying the server of the event concerning request information sent from the user terminal to another system when the event is detected,
- so that said step (c) in the server releases the session when the event is notified from
- 35 the step (g) in the user terminal.

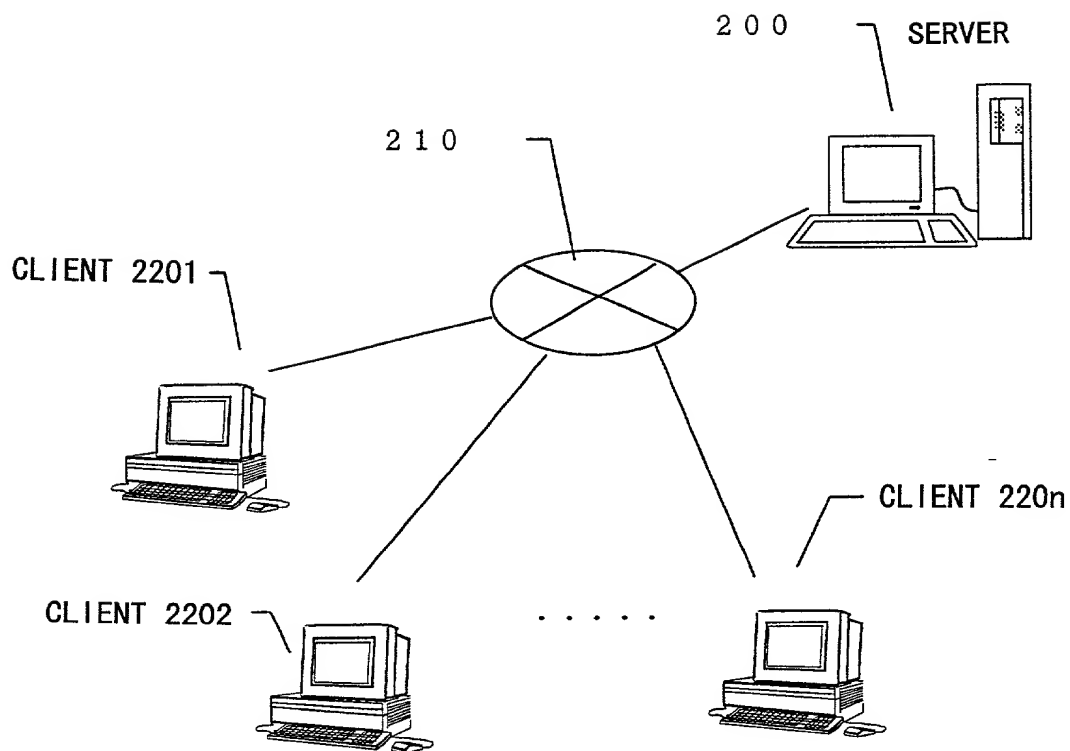
9. The method as claimed in claim 7,  
wherein said step (c) comprises the steps of sending  
5 a confirmation notification in a predetermined period  
to check whether the user terminal is connected  
through the session so that said step (c) manages the  
session in accordance with a response from the user  
terminal to the confirmation notification.  
10

10. The method as claimed in claim 7,  
15 wherein said step (c) manages the session based on  
whether the condition information is provided from  
the user terminal within a predetermined period or  
not.

ABSTRACT OF THE DISCLOSURE

In an information providing system, a condition notifying part is provided by a providing part to the user terminal with information that is in accordance with a request of the user terminal, is activated in a user terminal connecting to the information providing system via a network and notifies of a condition of the user terminal. In addition, a session management part manages session information in accordance with the condition of the user terminal notified by the condition notifying part activated in the user terminal. A session between the information providing system and the user terminal is established when the user is authenticated in accordance with authentication information from the user terminal and the session information managed by said session management part.

FIG.1



# FIG. 2 PRIOR ART

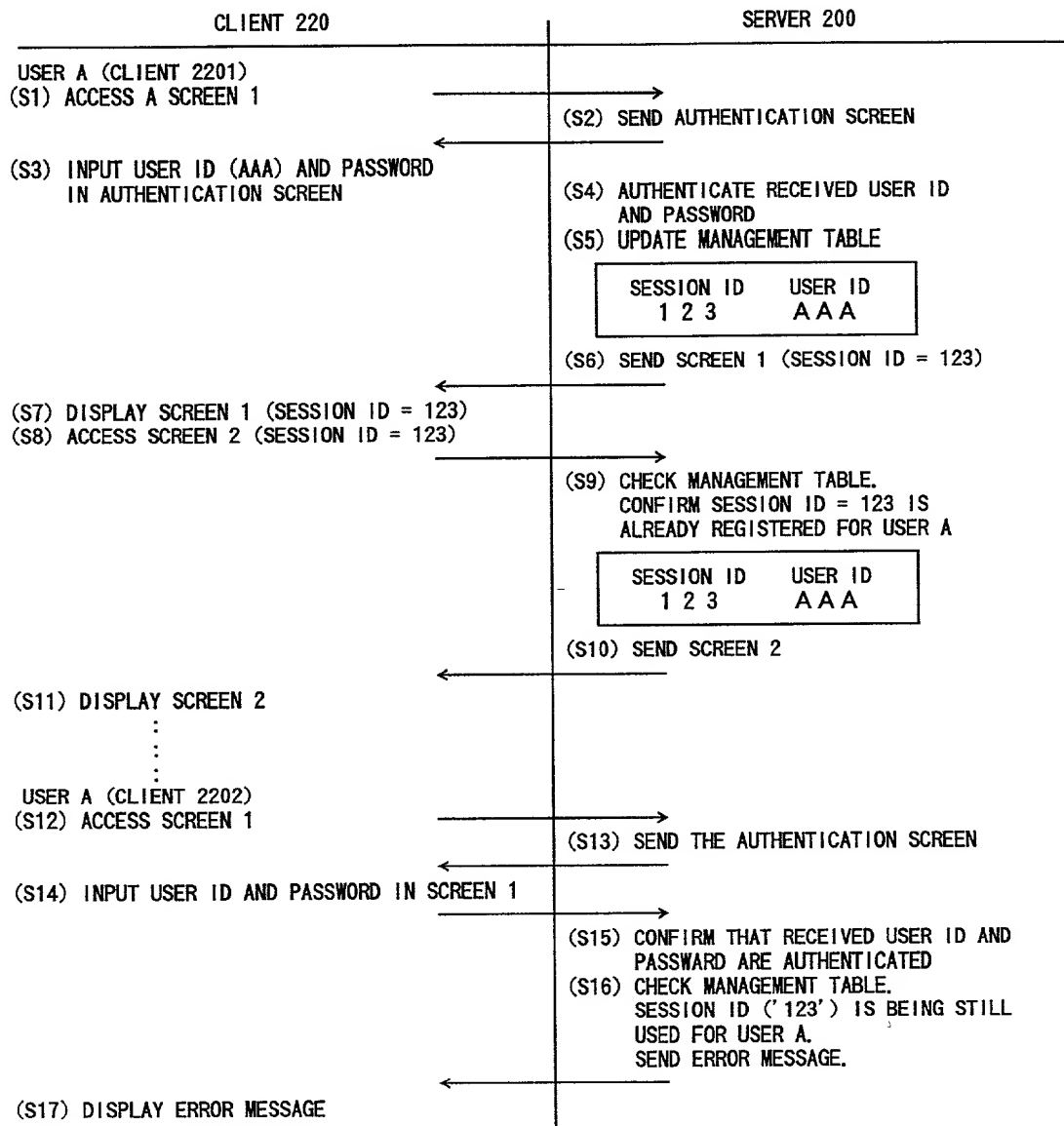
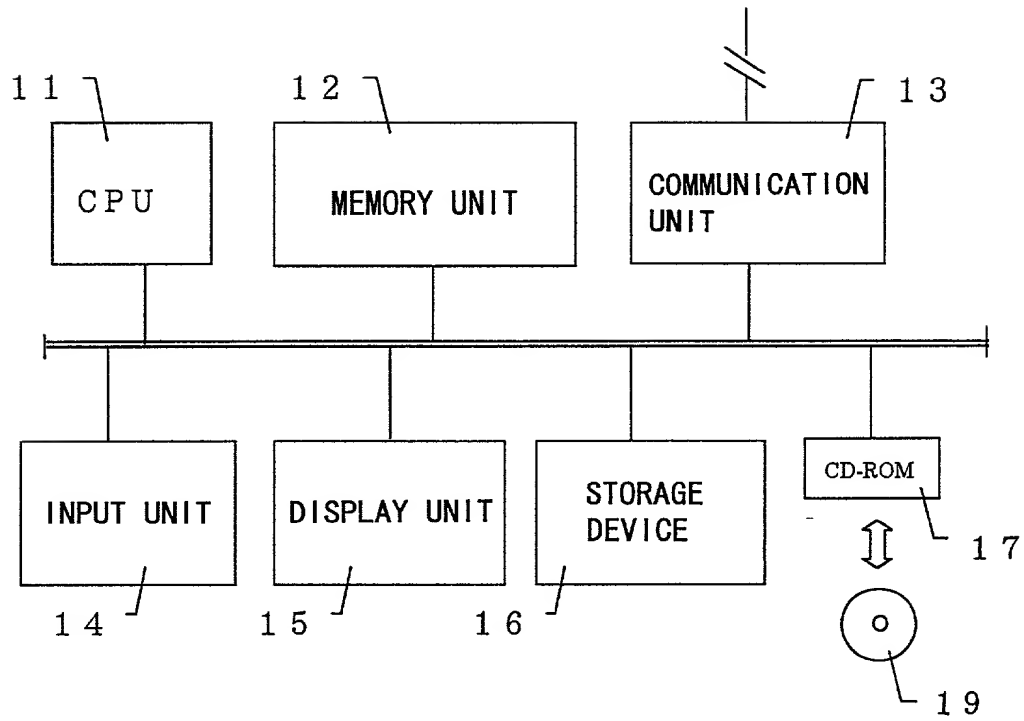
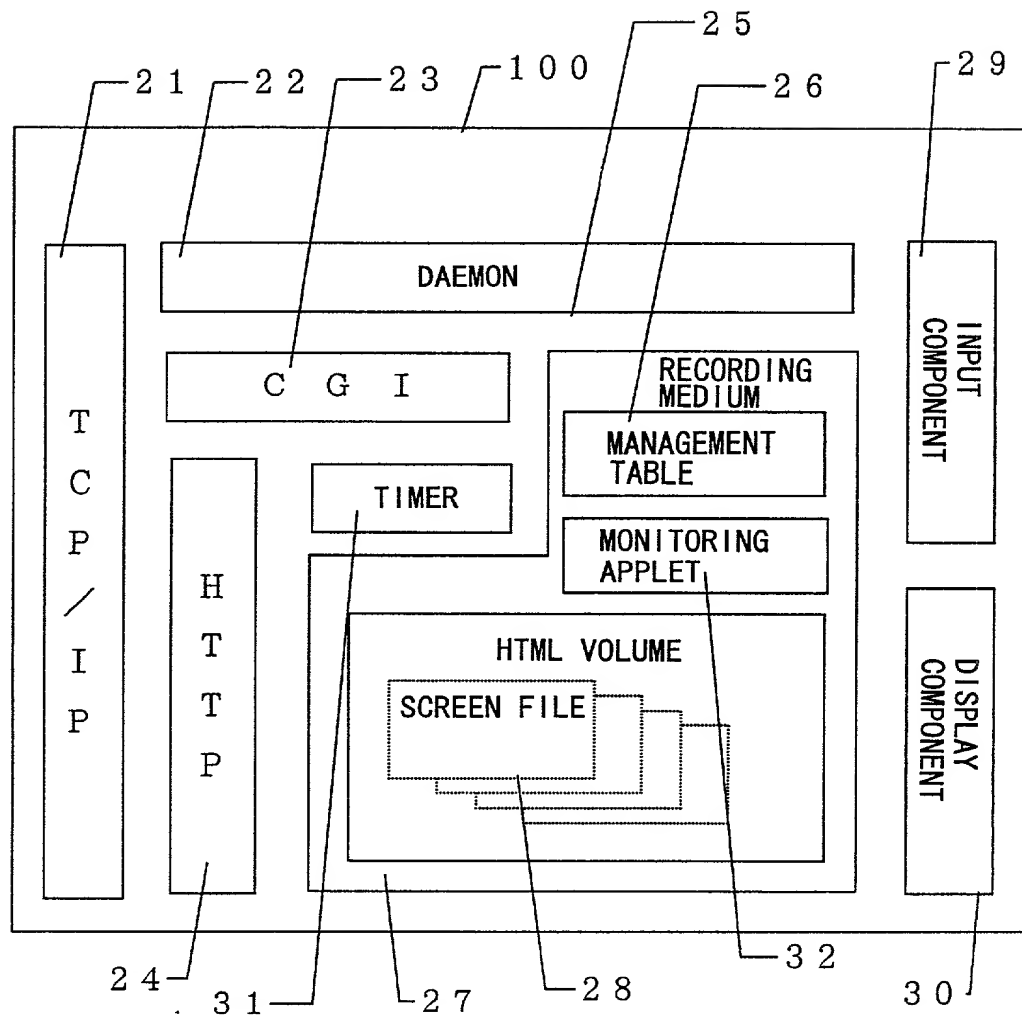


FIG.3

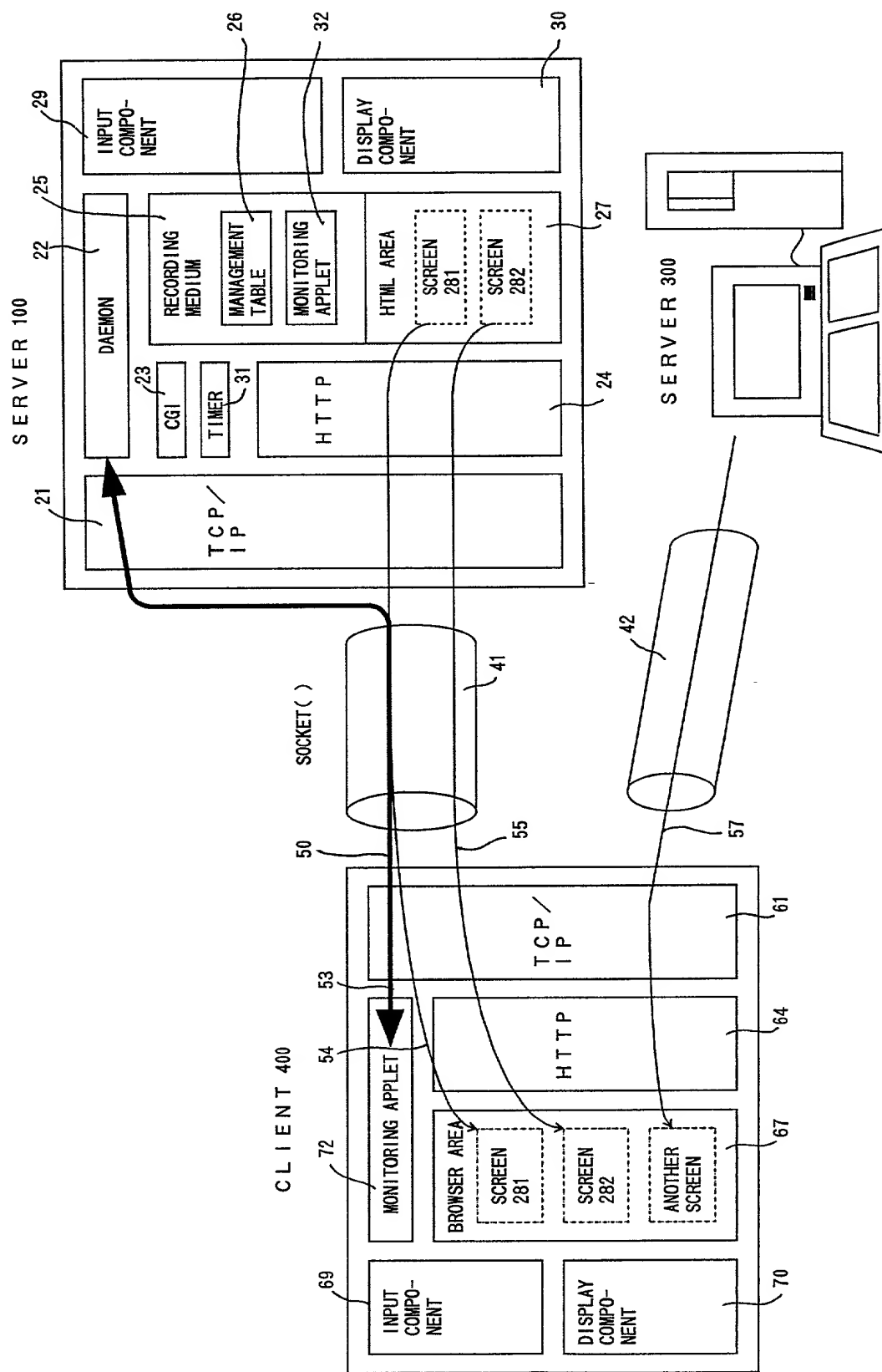


# FIG.4

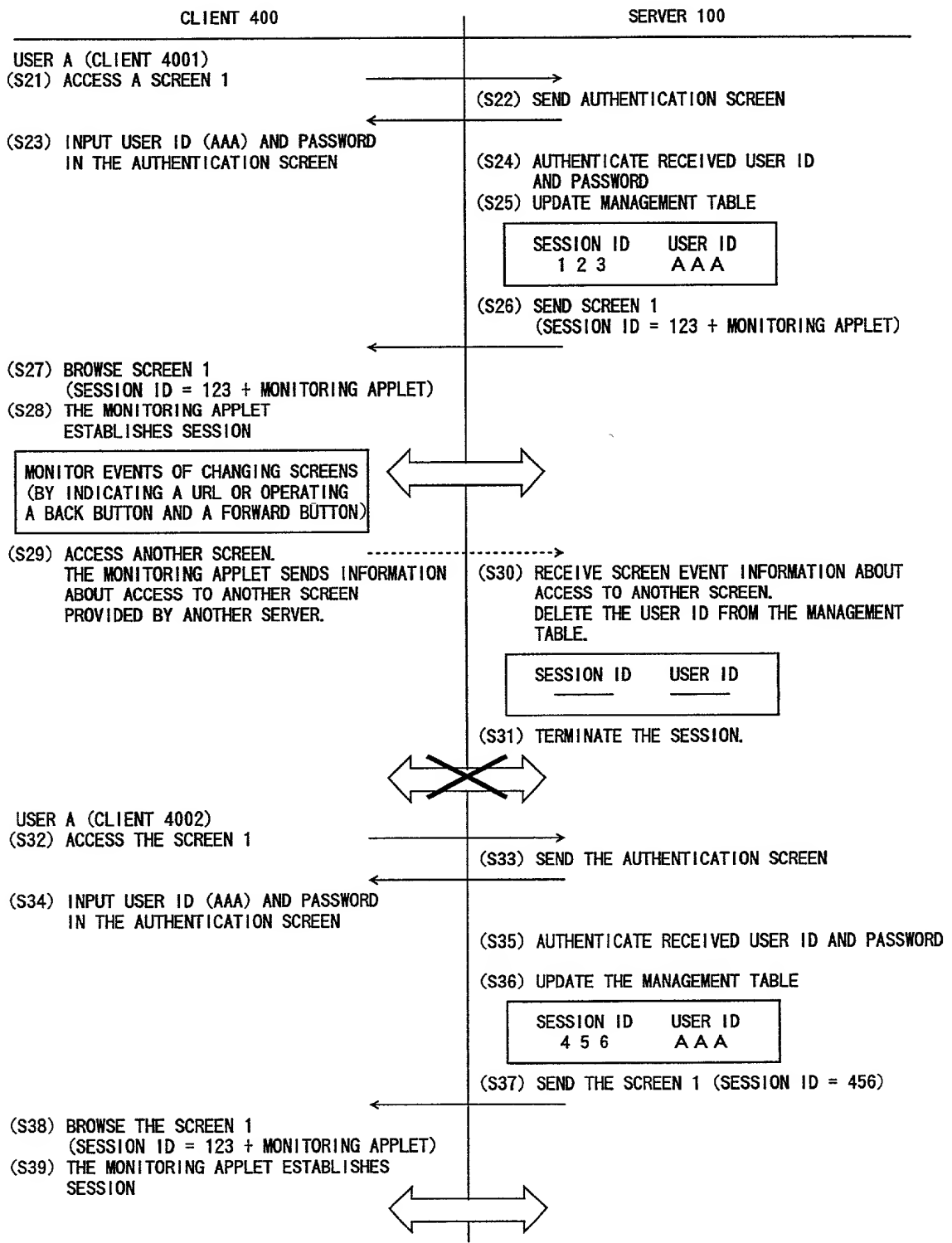




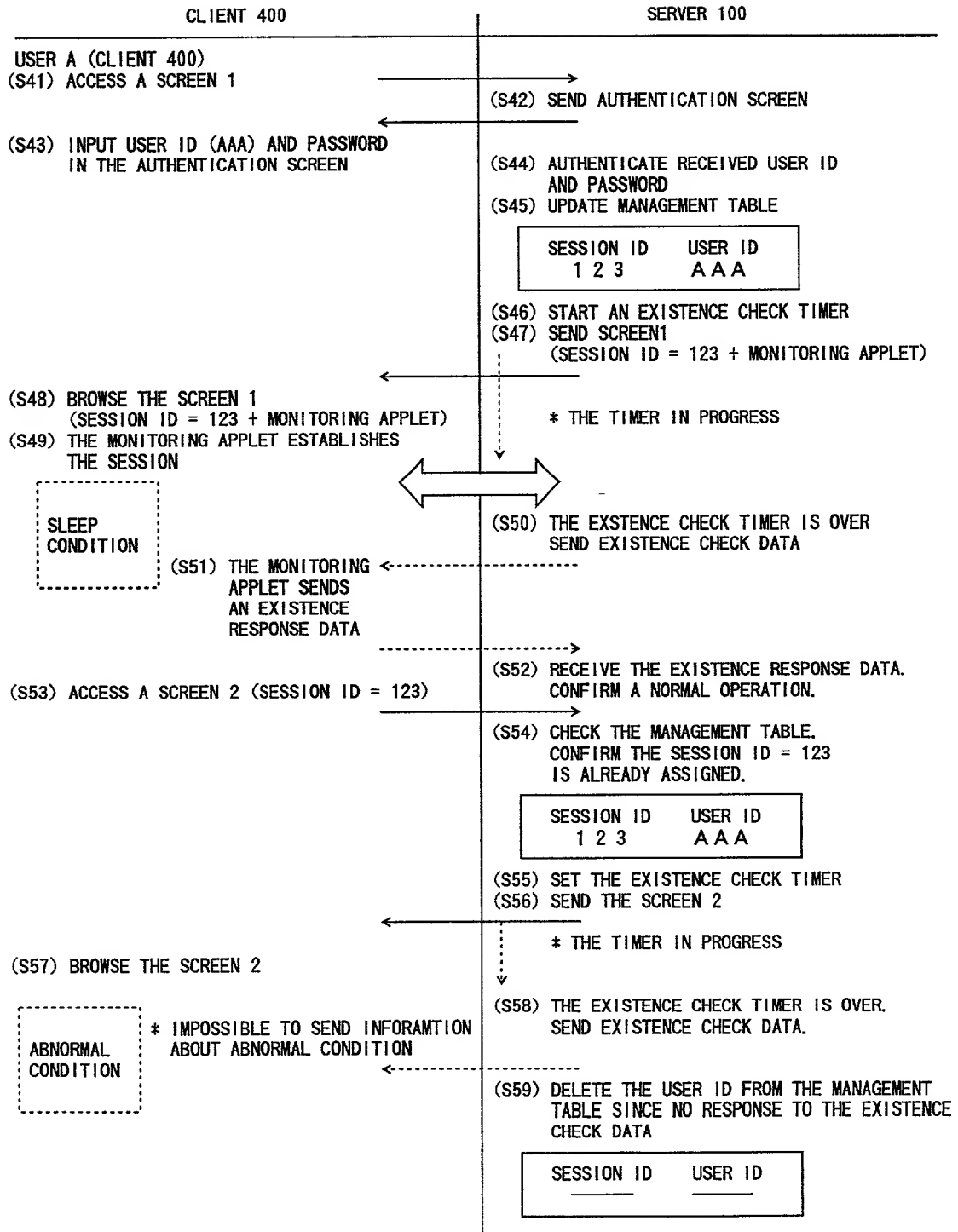
# FIG. 5



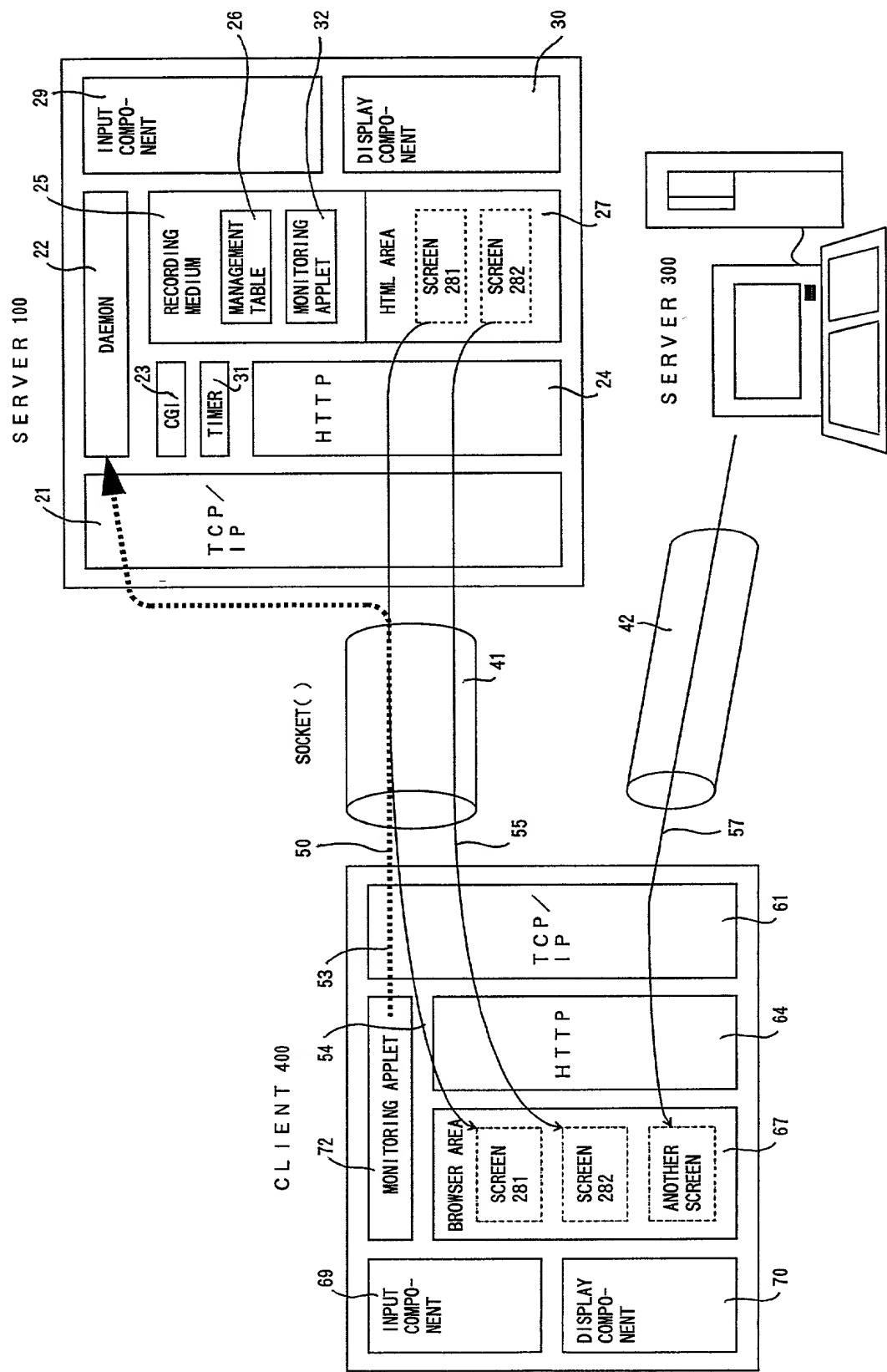
# FIG. 6



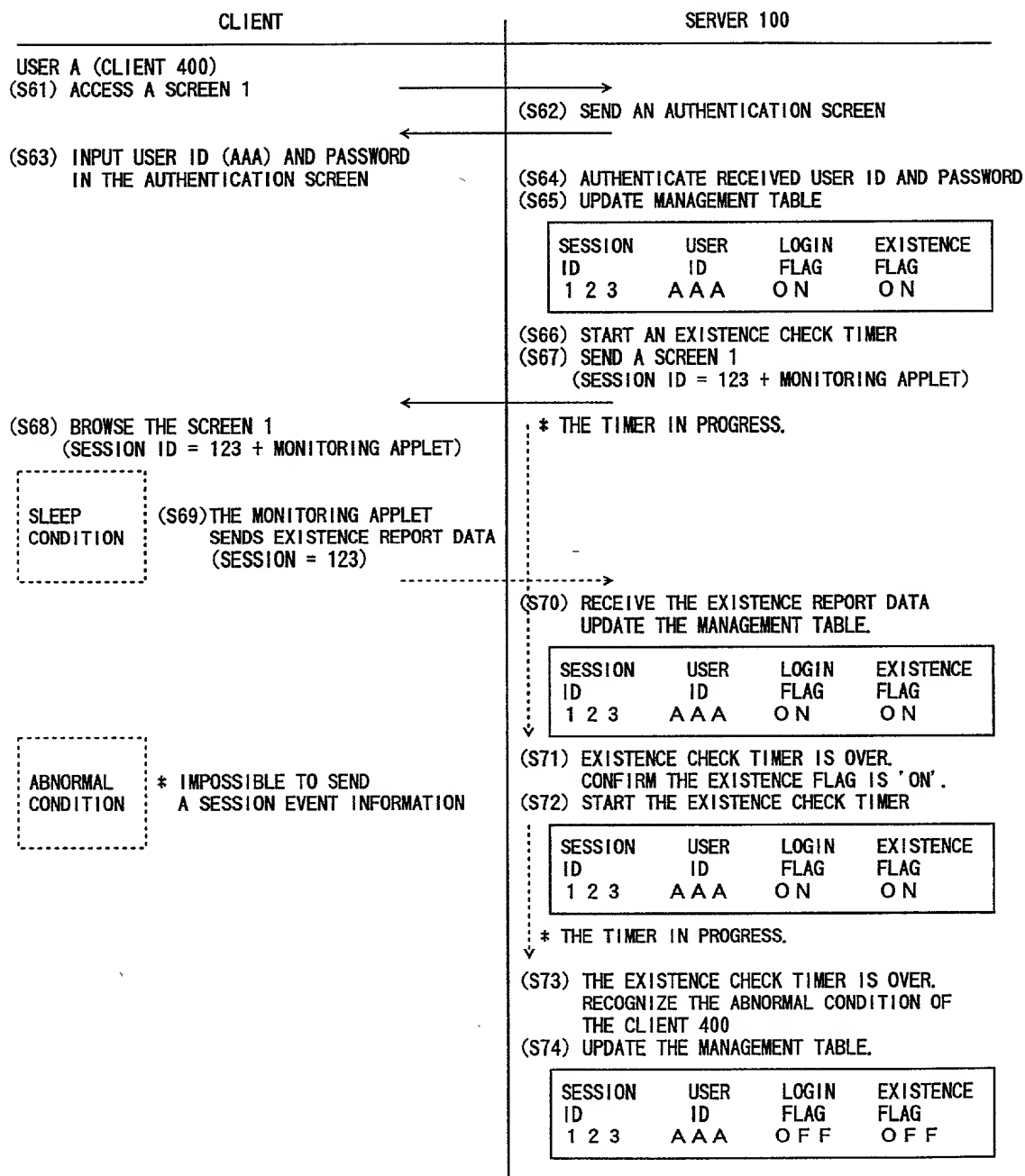
# FIG. 7



# FIG. 8



# FIG. 9



## Declaration and Power of Attorney For Patent Application

### 特許出願宣言書及び委任状

### Japanese Language Declaration

### 日本語宣言書

下記の氏名の発明者として、私は以下の通り宣言します。

As a below named inventor, I hereby declare that:

私の住所、私書箱、国籍は下記の私の氏名の後に記載された通りです。

My residence, post office address and citizenship are as stated next to my name.

下記の名称の発明に関して請求範囲に記載され、特許出願している発明内容について、私が最初かつ唯一の発明者（下記の氏名が一つの場合）もしくは最初かつ共同発明者であると（下記の名称が複数の場合）信じています。

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

#### INFORMATION PROVIDING SYSTEM AND

#### METHOD FOR PROVIDING INFORMATION

上記発明の明細書（下記の欄でX印がついていない場合は、本表に添付）は、

the specification of which is attached hereto unless the following box is checked:

☐ 月 日に提出され、米国出願番号または特許協定条約国際出願番号を \_\_\_\_\_ とし、  
（該当する場合） \_\_\_\_\_ に訂正されました。

☐ was filed on \_\_\_\_\_  
as United States Application Number or  
PCT International Application Number  
\_\_\_\_\_ and was amended on  
\_\_\_\_\_ (if applicable).

私は、特許請求範囲を含む上記訂正後の明細書を検討し、内容を理解していることをここに表明します。

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

私は、連邦規則法典第37編第1条56項に定義されるとおり、特許資格の有無について重要な情報を開示する義務があることを認めます。

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## Japanese Language Declaration (日本語宣言書)

私は、米国法典第35編119条(a)-(d)項又は365条(b)項に基づき下記の、米国外の国の少なくとも一カ国を指定している特許協力条約365(a)項に基づく国際出願、又は外国での特許出願もしくは発明者証の出願についての外国優先権をここに主張するとともに、優先権を主張している、本出願の前に出願された特許または発明者証の外国出願を以下に、枠内をマークすることで、示しています。

### Prior Foreign Application(s)

外国での先行出願 Pat. Appln. No. 10-365589	Japan
(Number) (番号)	(Country) (国名)
(Number) (番号)	(Country) (国名)

I hereby claim foreign priority under Title 35, United States Code, Section 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

### Priority Not Claimed

優先権主張なし

22/December/1998

(Day/Month/Year Filed)  
(出願年月日)

☐

(Day/Month/Year Filed)  
(出願年月日)

☐

私は、第35編米国法典119条(e)項に基づいて下記の米国外特許出願規定に記載された権利をここに主張いたします。

(Application No.) (出願番号)	(Filing Date) (出願日)
-----------------------------	------------------------

私は、下記の米国法典第35編120条に基づいて下記の米国外特許出願に記載された権利、又は米国外を指定している特許協力条約365条(c)項に基づく権利をここに主張します。また、本出願の各種米国外の内容が米国法典第35編112条第1項又は特許協力条約で規定された方法で先行する米国外特許出願に開示されていない限り、その先行米国外出願書提出日以降で本出願書の日本国内または特許協力条約国際提出日までの期間中に入手された、連邦規則法典第37編1条56項で定義された特許資格の有無に関する重要な情報について開示義務があることを認識しています。

(Application No.) (出願番号)	(Filing Date) (出願日)
-----------------------------	------------------------

(Application No.) (出願番号)	(Filing Date) (出願日)
-----------------------------	------------------------

私は、私自身の知識に基づいて本宣言書中で私が行なう表明が真実であり、かつ私の入手した情報と私の信じることに基づく表明が全て真実であると信じていること、さらに故意になされた虚偽の表明及びそれと同等の行為は米国法典第18編第1001条に基づき、罰金または拘禁、もしくはその両方により処罰されること、そしてそのような故意による虚偽の表明を行なえば、出願した、又は英に許可された特許の有効性が失われることを認識し、よってここに上記のごとく宣誓を致します。

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below.

(Application No.) (出願番号)	(Filing Date) (出願日)
-----------------------------	------------------------

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s), or 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of application.

(Status: Patented, Pending, Abandoned) (現況: 特許許可済、係属中、放棄済)
---

(Status: Patented, Pending, Abandoned) (現況: 特許許可済、係属中、放棄済)
---

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## Japanese Language Declaration (日本語宣言書)

委任状： 私は下記の発明者として、本出願に関する一切の  
手続を米特許商標局に対して遂行する弁理士または代理人  
として、下記の者を指名いたします。(弁護士、または代理  
人氏名及び登録番号を明記のこと)

POWER OF ATTORNEY: As a named inventor, I hereby appoint  
the following attorney(s) and/or agent(s) to prosecute this  
application and transact all business in the Patent and Trademark  
Office connected therewith (list name and registration number)

James D. Halsey, Jr., 22,729; Harry John Staas, 22,010; David M. Pitcher, 25,908; John C. Garvey, 28,607; J. Randall Beckers, 30,358;  
William F. Herbert, 31,024; Richard A. Gollhofer, 31,106; Mark J. Henry, 36,162; Gene M. Garner II, 34,172; Michael D. Stein, 37,240; Paul  
I. Kravetz, 35,230; Gerald P. Joyce, III, 37,648; Todd E. Marlette, 35,269; Harlan B. Williams, Jr., 34,756; George N. Stevens, 36,938;  
Michael C. Soldner, P-41,455 and William M. Schertler, 35,348 (agent)

送付先

Send Correspondence to:

STAAS & HALSEY  
700 Eleventh Street, N.W.  
Suite 500  
Washington, D.C. 20001

直接電話連絡先： (名前及び電話番号)

Direct Telephone Calls to: (name and telephone number)

STAAS & HALSEY  
(202) 434-1500

唯一または第一発明者名		Full name of sole or first inventor	
		Kenichi Yamamoto	
発明者の署名	日付	Inventor's signature	Date
		Kenichi Yamamoto	December 13, 1999
住所		Residence	
		Kawasaki-shi, Kanagawa, Japan	
国籍		Citizenship	
		Japan	
私書箱		Post Office Address	
		c/o FUJITSU LIMITED,	
		1-1, Kamikodanaka 4-chome, Nakahara-ku,	
		Kawasaki-shi, Kanagawa, 211-8588 Japan	
第二共同発明者		Full name of second joint inventor, if any	
		Hideaki Okada	
第二共同発明者	日付	Second inventor's signature	Date
		Hideaki Okada	December 13, 1999
住所		Residence	
		Maebashi-shi, Gunma, Japan	
国籍		Citizenship	
		Japan	
私書箱		Post Office Address	
		c/o FUJITSU TERMINAL SYSTEMS LIMITED,	
		8-3, Tonyamachi 1-chome, Maebashi-shi,	
		Gunma, 371-0855 Japan	

(第三以降の共同発明者についても同様に記載し、署名をす  
ること)

(Supply similar information and signature for third and subsequent  
joint inventors.)



第三共同発明者		Full name of third joint inventor, if any Teruo Nakazawa
第三共同発明者	日付	Third inventor's signature      Date <i>Teruo Nakazawa</i> December 13, 1999
住 所		Residence Maebashi-shi, Gunma, Japan
国 籍		Citizenship Japan
私書箱		Post Office Address c/o FUJITSU TERMINAL SYSTEMS LIMITED, 8-3, Tonyamachi 1-chome, Maebashi-shi, Gunma, 371-0855 Japan
第四共同発明者		Full name of fourth joint inventor, if any Hideki Mikamoto
第四共同発明者	日付	Fourth inventor's signature      Date <i>Hideki Mikamoto</i> December 13, 1999
住 所		Residence Ota-ku, Tokyo, Japan
国 籍		Citizenship Japan
私書箱		Post Office Address c/o FUJITSU FINANCIAL SYSTEMS LIMITED, 37-10, Nishikamata 7-chome, Ota-ku, Tokyo, 144-0051 Japan

第五共同発明者		Full name of fifth joint inventor, if any
第五共同発明者	日付	Fifth inventor's signature      Date
住 所		Residence
国 籍		Citizenship
私書箱		Post Office Address
第六共同発明者		Full name of sixth joint inventor, if any
第六共同発明者	日付	Sixth inventor's signature      Date
住 所		Residence
国 籍		Citizenship
私書箱		Post Office Address

(第七以降の共同発明者についても同様に  
記載し、署名をすること)

(Supply similar information and signature for  
seventh and subsequent joint inventors.)